UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
CHATTANOOGA DIVISION

ECOLAB INC., and NALCO COMPANY, LLC d/b/a Nalco Water, an Ecolab Company and/or Nalco Water, Plaintiffs, v. ANTHONY RIDLEY and CHEMTREAT, INC., Defendants.	No. 1:22-cv-00050-TRM-SKL Hon. Travis McDonough Magistrate Judge Susan K. Lee

EXPERT REPORT OF LAURENCE D. LIEB

Introduction

1. My name is Laurence D. Lieb. I am the President of Tyger Forensics Inc., which provides, among other things, computer forensics and electronic discovery services to litigation attorneys and their clients. I am a Magnet Forensics Certified Examiner and a Cellebrite Certified BlackLight Examiner. I am also a licensed private investigator in the State of Michigan.

2. To obtain my certification as a Magnet Forensics Certified Examiner, I undertook online training led by Magnet Forensics. To remain certified, I am required, from time to time, to retrain and pass certification examinations for new software versions. A true and exact copy of my certification is attached as part of **Exhibit A** and incorporated by reference.

3. To obtain my certification as a Cellebrite Certified BlackLight Examiner, I undertook online training led by Cellebrite. To remain certified, I am required, from time to time, to retrain and pass certification examinations for new software versions. A true and exact copy of my certification is attached as part of **Exhibit B** and incorporated by reference.

4. I counsel and assist clients in the preservation, extraction, and analysis of electronic data, using industry-standard practices, based on evidence personally analyzed, and form expert opinions regarding human interaction with electronic data from smartphones, computers, cloud-based sources, and a myriad of other electronic devices. I have been retained for this type of work around the country by numerous clients, as described in my curriculum vitae, which is attached as **Exhibit C**.

5. I have been retained by Ecolab, and its counsel, Fisher & Phillips LLP, to provide expert opinions regarding my forensic analysis of a data loss prevention system report and documents in the litigation titled ECOLAB Inc., and NALCO COMPANY, LLC d/b/a Nalco Water, an Ecolab Company and/or Nalco Water, Plaintiffs, v. ANTHONY RIDLEY, and

CHEMTREAT, INC, pending in the United States District Court, Eastern District of Tennessee, Chattanooga Division (the "Litigation").

6. My hourly rate for this matter varies by task as follows: for pure forensic analysis & reporting, $350 per hour; for written declarations, depositions, and other sworn testimony, $450 per hour. My fees are unrelated to the outcome of the Litigation. My curriculum vitae, attached as **Exhibit C**, lists my testimonial experience for the last four years and all my publications for the last ten years.

7. This report is based on my personal knowledge, experience, and expertise in the area of forensic analysis of electronic devices. It is also based on my review of the documents and information contained within Ecolab former employee, Anthony Ridley's OneDrive account and Ecolab's digital loss prevention tool, Digital Guardian's report which captured Anthony Ridley's human interaction with Ecolab's files, and ChemTreat's CrowdStrike report.

8. It is my understanding that the plaintiffs in this case are Ecolab, Inc. and Nalco Company, LLC ("Plaintiffs" or "Ecolab"), and the defendants are ChemTreat, Inc. ("ChemTreat") and a former employee of Plaintiff named Anthony Ridley ("Ridley"). The claims pleaded by the Plaintiff, include (1) theft of trade secrets in violation of the Defend Trade Secrets Act, (2) violation of the Tennessee Uniform Trade Secrets Act, (3) breach of contract, (4) breach of fiduciary duty of loyalty, (5) tortious interference with contractual relationships, (6) procurement of breach of contract, (7) unfair competition, and (8) civil conspiracy. Plaintiffs claim that Ridley misappropriated trade secrets and other confidential information from Ecolab.

9. I understand that discovery is ongoing in this Litigation. I reserve the right to render additional opinions, to supplement or amend the opinions in this report, and to provide additional grounds for those opinions based on my ongoing analysis of the materials provided to me or as may

be required by events that occur during the course of this Litigation, including but not limited to responding to or analyzing positions taken by Ridley or his experts.

Forensic Preservation

10. I used AccessData FTK Imager version 4.5.0.3 to create a bit for bit forensic image of Ridley's Ecolab Microsoft OneDrive account ("OneDrive Account").

11. It is critical to use "Best Practices" when conducting a forensic examination. "Best Practices" are defined as use of industry-standard chain of custody forensic software that will preserve and maintain which specific person has sole control over a specific single source of electronic evidence up to a time and date certain. It also includes the use of tools and methodologies that do not make changes to the underlying electronic evidence in any way. If the proper standardized software is not used, it can result in the underlying data being changed or otherwise distorted. The software, tools, and methodologies that I used to conduct my forensic examination comport with these "Best Practices."

Digital Guardian Report

12. Ecolab employs a data loss prevention tool, Digital Guardian, to journal Ecolab employees' interactions with Ecolab files, specifically to capture and memorialize unauthorized exfiltration of files, such as the downloading and copying of Ecolab files to external USB media, uploading of Ecolab files to non-Ecolab cloud storage services, and the emailing of Ecolab files to 3rd party email accounts. Digital Guardian is designed specifically to record the exfiltration of trade secrets, intellectual property and company files by employees. Furthermore, the Digital Guardian Report contains all the categories of information I seek to analyze and report on in theft of trade secrets matters. The fact that I was not able to forensically analyze Ridley's former Ecolab work computers has literally no effect on my strongly held opinion that Ridley exfiltrated thousands of Ecolab files.

13. Ecolab's data loss prevention tool, Digital Guardian version 8.4.0.0263, generated a report ("Digital Guardian Report") of all interactions former employee Ridley performed regarding Ecolab files during the period May 22, 2021 through July 1, 2021 inclusive. I forensically analyzed the Digital Guardian Report and came to the forensic observations and opinions set forth in this report.

14. The Digital Guardian Report captured and recorded an extensive amount of files being exfiltrated by Ridley using his former Ecolab laptop. From a forensic analysis standpoint, the Digital Guardian Report provides more than sufficient amount of information for me to arrive at my conclusion that Ridley misappropriated thousands of Ecolab files.

Forensic Analysis – Uploading Files to a Personal Microsoft Account

15. Forensic analysis revealed Ridley uploading a file named "fb na sales 2021 exprice review for customers.pptx" to a personally owned Microsoft account on **5/22/2021 10:05 PM EST** from Ridley's Ecolab workstation, an HP 1030 G2.

16. Forensic analysis revealed Ridley uploading a file named "2021 partnership and market overview.pptx" to a personally owned Microsoft account on **5/22/2021 10:20 PM EST** from Ridley's Ecolab workstation, an HP 1030 G2.

17. Forensic analysis revealed Ridley uploading a file named "2021 partnership and market overview - [redacted].pptx" to a personally owned Microsoft account on **5/22/2021 10:32 PM EST** from Ridley's Ecolab workstation, an HP 1030 G2.

18. Forensic analysis revealed Ridley uploading a file named "intensive cleaning procedure covid 19 goggles.docx" to a personally owned Microsoft account on **5/24/2021 11:10 AM EST** from Ridley's Ecolab workstation, an HP 1030 G2.

19. Forensic analysis revealed Ridley uploading a file named "notes for [redacted] 2006 contract.doc" to a personally owned Microsoft account on **5/24/2021 1:12 PM EST** from Ridley's Ecolab workstation, an HP 1030 G2.

20. Forensic analysis revealed Ridley uploading a file named "esisting (*sic*) inventory quote.doc" to a personally owned Microsoft account on **5/24/2021 1:12 PM EST** from Ridley's Ecolab workstation, an HP 1030 G2.

21. Forensic analysis revealed Ridley uploading a file named "2021 [redacted] example rfp purchase agreement - october 2020.docx" to a personally owned Microsoft account on **6/8/2021 10:55 AM EST** from Ridley's Ecolab workstation, an HP 1030 G2.

22. Forensic analysis revealed Ridley uploading a file named "[redacted] monthly tracking report 06-2021.xlsx" to a personally owned Microsoft account on **6/18/2021 10:13 PM EST** from Ridley's Ecolab workstation, an HP 1030 G2.

23. I understand that ChemTreat terminated Ridley in March 2022, purportedly after its investigation uncovered the fact that Ridley had emailed an Ecolab file from his personal Microsoft email account to his ChemTreat email account in September 2021. This is consistent with my analysis of the Digital Guardian Report, which uncovered evidence of Ridley uploading Ecolab files to his personal Microsoft account as documented in paragraphs 15 through 22 above.

24. It is my opinion that Ridley exfiltrated the many Ecolab files documented in this report specifically to utilize them while employed at ChemTreat.

Forensic Analysis – Downloading Files to an External LaCie USB Drive

25. Forensic analysis revealed Ridley downloading and copying a significant number of documents and Ecolab data to two separate external USB drives in the two months prior to Ridley's resignation from Ecolab. I have been informed that Ridley's last date of employment at Ecolab was July 1, 2021.

26. Forensic analysis revealed Ridley exporting a file named "ridley contacts.csv" from Ridley's Ecolab Microsoft Outlook account to an external USB drive, USB Association VendorID 090c, serial number 416000000000000, on 6/21/2021 3:36:00 PM.

27. Forensic analysis revealed Ridley downloading and copying the 9,741 files and folders listed in **Exhibit** D to a removable LaCie brand USB drive ("LaCie Drive"), serial number def10dce9db4, on 6/1/2021.

28. Forensic analysis revealed Ridley downloading and copying the 149 files and folders listed in **Exhibit** E to the LaCie Drive on 5/27/2021.

29. Forensic analysis revealed Anthony Ridley downloading and copying the 185 files and folders listed in **Exhibit** F to the LaCie brand USB drive on 5/26/2021.

30. Forensic analysis revealed Anthony Ridley downloading and copying the 1,798 files and folders listed in **Exhibit** G to the LaCie brand USB drive on 5/25/2021.

31. Forensic analysis revealed Anthony Ridley downloading and copying the 4,891 files and folders listed in **Exhibit** H to the LaCie brand USB drive on 5/24/2021.

Forensic Analysis of Three USB Drives

32. I was provided with three USB drives belonging to Ecolab which Anthony Ridley kept after his employment with Ecolab ended. I further understand that Ridley returned these drives to Ecolab after Ecolab's counsel demanded that they be returned. In fact, these three drives were sent to me directly by Ridley's counsel. Upon receipt of the drives, I generated industry standard bit-for-bit forensic images of each drive. The makes, models and serial numbers of the three USB drives are listed below in Table 1 and are incorporated herein by reference.

Table 1 – Three USB Drives

EVIDENCE #	MAKE/MODEL	SERIAL NUMBER
USB001	UDisk	6&25676984&0&_&0

USB002	USB Flash Disk	0416080000012762 Revision: 1100
USB003	USB DISK 2.0	910101099030

33. Forensic analysis revealed that Anthony Ridley created a folder on drive USB001 named "Files from Ridley's personal computer" on 2/9/2022 3:34:01 PM, which I understand was after Mr. Ridley received a cease-and-desist letter from Ecolab's counsel earlier that same day.

34. Forensic analysis revealed a file named "_esktop.ini" on drive USB001 with a file creation date of 2/9/2022 3:34:01 PM. "_esktop.ini" is a Windows system file which normally is only found in the desktop folder of a Windows computer. Therefore, it is my expert opinion that Anthony Ridley copied this "_esktop.ini" file from a Windows computer's desktop folder to drive USB001 on 2/9/2022 3:34:01 PM.

35. Forensic analysis revealed multiple deleted files on drive USB001. A complete list of the deleted folders and files recovered from drive USB001 is listed below as Table 2 and is incorporated herein by reference. In my opinion, Mr. Ridley deleted the files listed below in Table 2 in a failed attempt to hide the fact that the drive contained Ecolab files.

Table 2 – Deleted Folders and Files Recovered from Drive USB001

Deleted Folder or File Name	Location on Drive USB001
_ESKTOP.INI	USB001:\Files from Ridley's personal computer\Music\
_ESKTOP.INI	USB001:\Files from Ridley's personal computer\Pictures\
Sales Plan Strategies.pdf	USB001:\Sales Planning Tools\Planning Guides\
[redacted] Boiler Operator Training Final 4kwk.ppt	USB001:\
Proposal for [redacted] Program 121417EC (002) - December 2017.pdf	USB001:\
~$[redacted] Boiler Operator Training Final 4kwk.ppt	USB001:\
Sales Tactics.pdf	USB001:\Sales Planning Tools\Planning Guides\
[redacted] Boiler Operator Training Final 4kwk.ppt	USB001:\
~$[redacted] Boiler Operator Training Final 4kwk.ppt	USB001:\
Call Planner (Pads).docx	USB001:\Sales Planning Tools\Sales Plans\
Sales Plan Overview.docx	USB001:\Sales Planning Tools\Sales Plans\

Activity Log.docx	USB001:\Sales Planning Tools\Sales Plans\
Target Account Assessment.docx	USB001:\Sales Planning Tools\Sales Plans\
_.H2W	USB001:\
Sales Planning Tools	USB001-ANTHONY-RIDLEY.E01\Root\Sales Planning Tools\
Planning Guides	USB001-ANTHONY-RIDLEY.E01\Root\Sales Planning Tools\Planning Guides\
Sales Plans	USB001-ANTHONY-RIDLEY.E01\Root\Sales Planning Tools\Sales Plans\

36. Forensic analysis revealed Anthony Ridley's deletion of a file named "[redacted] Boiler Operator Training Final 4kwk.ppt" from drive USB001 on 02/09/2022.

37. Forensic analysis revealed Anthony Ridley's deletion of a file named "Sales Plan Strategies.pdf" from drive USB001 on 02/09/2022.

38. Forensic analysis revealed Anthony Ridley's deletion of a folder named "Planning Guides" from drive USB001 on 02/09/2022.

39. Forensic analysis revealed Anthony Ridley's deletion of a file named "Ridley Contacts.CSV" from drive USB002 on 02/09/2022. In fact, this "Ridley Contacts.CSV" appears to be the exact same file Ridley exfiltrated from Ecolab on 6/21/2021 3:36:00 PM as memorialized in the Digital Guardian Report.

40. Therefore, it is my expert opinion that Ridley attempted, but failed to hide the fact that he was in possession of the above-mentioned Ecolab files.

Forensic Analysis of the Anthony Ridley OneDrive Account

41. Forensic analysis of Ridley's Ecolab OneDrive account uncovered the fact that Ridley exfiltrated and then destroyed a significant number of Ecolab files in an attempt to deprive his former employer access to these same files.

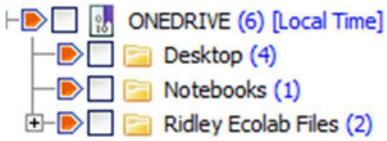
42. I first made a forensic image of Anthony Ridley's Ecolab OneDrive account contents using AccessData's FTK Imager version 4.5.0.3 to enable forensic analysis of this evidence.

43. Forensic analysis of the Ridley OneDrive account forensic image revealed the fact that, after downloading and copying the folders and files described above in paragraphs 23 through 29, Anthony Ridley deleted all these same folders and files from his Ecolab OneDrive account.

44. Forensic analysis revealed the fact that Ridley's Ecolab OneDrive account originally held four top level folders, named "Desktop", "Notebooks", "Ridley's Ecolab Files" and "ridley's nalco folder" respectively.

45. The screenshot below from my forensic tool shows the current top level folder structure of Ridley's OneDrive account at the time I created a forensic image of the account. Forensic analysis revealed the fact that all the folders and files Ridley deleted from his Ecolab OneDrive account existed under a single the top-level folder named "ridley's nalco folder." This now deleted "ridley's nalco folder" folder would have existed in the screenshot below immediately under the "Ridley Ecolab Files" folder but for the fact that Ridley deleted the "ridley's nalco folder" folder from his Ecolab OneDrive account after downloading the "ridley's nalco folder" folder and the folder's contents to the LaCie drive.

Screenshot of Ridley OneDrive Account at time of Forensic Collection Showing Missing and Deleted "ridley's nalco folder"



46. Forensic analysis revealed the fact that Ridley deleted the top level "ridley's nalco folder" after uploading the three files identified in paragraphs 15, 16 and 17 to Ridley's personal Microsoft cloud account.

47. Forensic analysis revealed the fact that prior to Ridley's deletion of the top level "ridley's nalco folder," Ridley's entire Ecolab OneDrive account contained 18 gigabytes of files.

48. I have been informed that Ridley asserts that he deleted the files in order to "declutter" his OneDrive account. It is my opinion that there was absolutely no need to "declutter" his OneDrive account, but in fact this act of deletion was designed to deprive Ecolab access to these same files.

49. I have been informed that ChemTreat wiped beyond recovery all content of Anthony Ridley's ChemTreat work computer. Forensic analysis of the Ridley ChemTreat work computer before it was wiped could have revealed evidence of Ridley downloading Ecolab files to his ChemTreat work computer from Ridley's personal Microsoft account and evidence of Ridley accessing and copying information from the exfiltrated Ecolab files stored within Ridley's personal Microsoft account to newly created ChemTreat files.

50. Therefore, in my opinion, and all evidence is consistent with the fact that Ridley exfiltrated thousands of Ecolab files and then deleted those same files to deprive Ecolab access to them.

ChemTreat's CrowdStrike Report - CHEMR-000002195.XML

51. I was provided with a document produced by ChemTreat labeled as CHEMR-000002195.xml, which represents a CrowdStrike report containing some actions performed by Anthony Ridley while employed at ChemTreat. I performed a forensic analysis of CHEMR-000002195.xml and discovered the following evidence.

Missing AmazonBasics USB Drive Serial Number 180129000600

52. Forensic analysis of the CrowdStrike report revealed the fact that Anthony Ridley disconnected an AmazonBasics external USB drive, serial number 180129000600, on 2021-07-09 T10:21:37.103+0000 ("UTC") from his ChemTreat laptop.

CHEMR-000002195.XML CrowdStrike Report Reveals an AmazonBasics USB Drive

```
</result>
<result offset='1500102'>
    <field k='_time'>
        <value><text>2021-07-09T10:21:37.103+0000</text></value>
    </field>
    <field k='name'>
        <value><text>DcUsbDeviceDisconnectedV2</text></value>
    </field>
    <field k='DeviceManufacturer'>
        <value><text>AmazonBasics</text></value>
    </field>
    <field k='DeviceProduct'>
        <value><text>AmazonBasics Hard Drive Enclos</text></value>
    </field>
    <field k='DeviceSerialNumber'>
        <value><text>180129000600</text></value>
    </field>
```

53. As of the date of this Expert Report, I have not been provided with a forensic image of this particular USB drive.

Ridley Accessed His Personal Microsoft Account Using His ChemTreat Laptop

54. Forensic analysis of CHEMR-000002195.xml identified the fact that Anthony Ridley accessed his personal Microsoft account by visiting "cdn.odc.officeapps.live.com" on 2021-10-30 T21:20:51.298+0000 (UTC). Live.com is Microsoft's website for individual, non-organizational customers of Microsoft online email and document storage services.

55. Forensic analysis revealed that less than one minute later, Ridley accessed a file named "EMS-103A Empty Container Requirements.docx" in his ChemTreat OneDrive folder named "Arnold Air Force Base\HVAC bid - 2021\" at 2021-10-30 T21:21:14.030+0000 ("UTC").

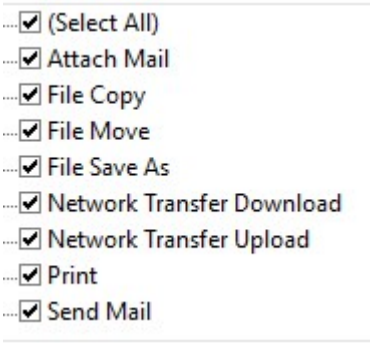
56. It is my opinion that this is evidence of Ridley accessing the exfiltrated Ecolab files from his personal Microsoft OneDrive account in order to use the content of the exfiltrated files.

57. Arnold Air Force Base was one of the customers whose files were uploaded by Ridley to his personal Microsoft account from Ridley's former Ecolab work computer on May 24, 2021.

58. In my opinion, the CrowdStrike tool, unlike the Digital Guardian tool, is not a data loss prevention tool. In fact, I spoke with three CrowdStrike representatives on February 7, 2023 who confirmed the fact that CrowdStrike does not hold itself out to be a data loss prevention tool developer. The CrowdStrike representatives stated that developing and offering a data loss prevention tool is planned for the future.

59. For example, the Digital Guardian tool recorded many types of human file interaction commonly used by employees to exfiltrate data as seen in the screenshot below. In contrast, the CrowdStrike tool does not record "attaching mail", "Network Transfer Download", "Network Transfer Upload", "Print", or "Send Mail".

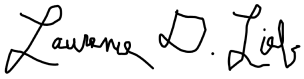
Digital Guardian Human Activity Recorded



60. Forensic analysis of the now wiped ChemTreat laptop would have provided the detail as to which specific exfiltrated Ecolab files Ridley was accessing from his personal Microsoft OneDrive account while interacting with the related ChemTreat files. Therefore, searches for the exfiltrated Ecolab file names within ChemTreat's email and OneDrive system alone will not uncover the Ecolab information Ridley used to while employed at ChemTreat.

Dated: February 24, 2022

Respectfully submitted,



_____
Laurence D. Lieb